WHAT IS CLAIMED IS:

1. A method of displaying data related to an intrusion event on a computer system, comprising:

capturing data related to the intrusion event;

decoding the captured data from a first predetermined format to a second predetermined format decipherable by humans, the decoded data comprising data components of intrusion signature, data summary, and detailed data;

correlating data components of the intrusion signature, data summary and detailed data to one another;

retrieving an web browser-based template; and

graphically displaying the correlated decoded data components using the web browser-based template.

2. The method, as set forth in claim 1, wherein graphically displaying the correlated decoded data components comprises graphically highlighting correlated data components of intrusion signature, data summary and detailed data using the web browser-based template.

3. The method, as set forth in claim 1, wherein graphically displaying the correlated decoded data components comprises:

receiving a user input selecting a displayed data component; and

graphically highlighting data components correlated to the selected data component using the web browser-based template.

4. The method, as set forth in claim 1, wherein graphically displaying the correlated decoded data comprises:

receiving a user input selecting a displayed data component;

graphically highlighting the user selected data component using the web browser-based template; and

graphically highlighting data components correlated to the selected data component using the web browser-based template.

5. The method, as set forth in claim 1, wherein capturing data comprises capturing network data packets of the intrusion event.

6. The method, as set forth in claim 1, wherein decoding the captured data comprises decoding the captured data from a binary format to a human-readable text format.

7. The method, as set forth in claim 1, wherein decoding the captured data comprises decoding the captured data to decoded data having a data link layer protocol header, a network layer protocol header, a network layer protocol data summary, and packet data in hexadecimal format.

8. The method, as set forth in claim 1, wherein decoding the captured data comprises decoding the captured data to decoded data having an Ethernet header, an IP header, an IP data summary, and packet data in hexadecimal format.

9. A method of displaying data of an intrusion detection system, comprising:

capturing, from a network, data related to an intrusion event in response to detecting an intrusion signature in the network data;

decoding the captured data from a predetermined format to a human-readable format, the decoded data comprising data components of network header data, data summary, and detailed data;

determining a correlation relationship between the data components of the intrusion signature, network header data, data summary and detailed data to one another; and

displaying the correlated decoded data components by using a web browser-based template.

10. The method, as set forth in claim 9, wherein graphically displaying the correlated decoded data comprises:

receiving a user input selecting a displayed data component; and

graphically highlighting all data components correlated to the selected data component using an HTML template.

11. The method, as set forth in claim 9, wherein graphically displaying the correlated decoded data comprises:

receiving a user input selecting a displayed data component;

graphically highlighting the user selected data component; and

graphically highlighting data components correlated to the selected data component.

12. The method, as set forth in claim 9, wherein capturing data comprises capturing network data packets of the intrusion event in response to detecting the presence of a predetermined data pattern in the network data packet.

13. The method, as set forth in claim 9, wherein decoding the captured data comprises decoding the captured data from a binary format to a text format.

14. The method, as set forth in claim 9, wherein decoding the captured data comprises decoding the captured data to decoded data having a data link layer protocol header, a network layer protocol header, a network layer protocol data summary, and packet data in hexadecimal format.

15. The method, as set forth in claim 9, wherein decoding the captured data comprises decoding the captured data to decoded data having an Ethernet header, an IP header, an IP data summary, and packet data in hexadecimal format.

16. A system of presenting data of an intrusion detection system, comprising:

a network driver capturing data related to an intrusion event upon detecting a predetermined intrusion signature;

a decode engine decoding the captured data from a predetermined format to a predetermined format decipherable by humans, the decoded data comprising data components of intrusion event data, data summary, and detailed data; and

a user interface graphically correlating data components of the intrusion signature, intrusion event data, data summary and detailed data to one another and displaying the correlated decoded data components according to a web browser-based format.

17. The system, as set forth in claim 16, wherein the user interface graphically highlights correlated data components of intrusion event data, data summary and detailed data using an HTML template.

18. The system, as set forth in claim 16, wherein the user interface is operable to receive a user input selecting a displayed data component, and graphically highlights all data components correlated to the selected data component using a web-based display template.

19. The system, as set forth in claim 16, further comprising a web server operable to transmit a file in a web-browser displayable format having the correlated and decoded data components.

20. The system, as set forth in claim 16, wherein the network driver captures network data packets of the intrusion event in response to the intrusion detection system detecting a predetermined data pattern corresponding to the predetermined intrusion signature.

21. The system, as set forth in claim 16, wherein the decode engine decodes the captured data from a binary format to a human-readable text format.

22. The system, as set forth in claim 16, wherein the decode engine decodes the captured data to decoded data components having a data link layer protocol header, a network layer protocol header, a network layer protocol data summary, and packet data in hexadecimal format.

23. The system, as set forth in claim 16, wherein the decode engine decodes the captured data to decoded data components having an Ethernet header, an IP header, an IP data summary, and packet data in hexadecimal format.